Advances in Artificial Intelligence and Machine Learning; Research 4 (2) 2276-2289 Received 29-02-2024; Accepted 20-05-2024; Published 27-05-2024

Application of Blockchain in Managing Security Challenges Confronting the Adoption of 4IR in Smart Environments

Maneo Ntseliseng Ramahlosi ramahlosi@gmail.com
Department of Information Technology
Central University of Technology
South Africa

Adeyinka Akanbi aakanbi@cut.ac.za
Department of Information Technology
Central University of Technology
South Africa

Corresponding Author: Maneo Ntseliseng Ramahlosi

Abstract

Occurrences of hacking intentions and privacy violations make digital trust a major challenge. This is true in the smart environment domain, where captured or recorded datasets serve as inputs for predictions and monitoring systems and must comply with many regulations due to the sensitivity of the predictions. This study explores how the application of Blockchain technology/solution, could be used to manage or mitigate the security challenges comforting smart environments and by extension a multi-hazard early warning system. In this paper, the security concerns from the adoption of smart environments are discussed and the mitigating factors are presented. The proposed model utilizes the inherent security features of Blockchain technology to address the security and privacy concerns that arise in data pipelines. The model is designed to ensure data integrity, confidentiality, and authenticity in a decentralized manner. The model is evaluated in a hybrid environment using a prototype implementation and simulation experiments with outcomes that demonstrate advantages over traditional approaches for a tamper-proof and immutable data pipeline for data authenticity and integrity using a confidential ledger.

Keywords: Security challenges, Internet of Things (IoT), 4IR, Blockchain, Data pipelines.

1. INTRODUCTION

In our digital world, access to personal and public data has become an item of concern, with challenging security and privacy aspects. This heightened concern is germane for every digital application or information system. Over the years, advancement in technologies has led to a geometric improvement in terms of the miniaturability and capability of monitoring devices, fueling the adoption move from primordial legacy systems to the Internet of Things (IoT) smart devices. Recently, 4IR technologies such as the IoT has spurred the growth of smart environments, allowing

Citation: Maneo Ntseliseng Ramahlosi and Adeyinka Akanbi. Application of Blockchain in Managing Security Challenges Confronting the Adoption of 4IR in Smart Environments. Advances in Artificial Intelligence and Machine Learning. 2024;4(2):131.

users to better understand, monitor and control their environment through a range of ubiquitous interconnected devices [1]. Advances in smart environment monitoring systems using IoT and sensors and keeping legacy systems up to date in a world of increasing cyber threats has always been a concern [2]. The cyber security challenges in the IoT era. In Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. These systems tend to have inherent security vulnerabilities and are often not compatible with security features and lack sufficient encryption methods. Hence, the security challenges persist despite the adoption and implementation of 4IR technologies.

With this paradigm shift to the IoT era, the focus is more on the integration of devices, interoperability of the technologies/systems, miniaturability and ubiquity of the devices rather than addressing the security vulnerability of the endpoint solutions. As a case study, sub-systems such as an EWS of an integrated multi-hazard early warning systems are not an exception, due to the reliance on the adoption of legacy systems and integration of 4IR technologies-based heterogeneous devices and systems (FIGURE 1). The study hypothesizes that the application of Blockchain solutions will secure the data pipeline necessary for a multi-hazard early warning system (MHEWS). The main aim of this study is on exploring how the application of Blockchain technology or solution, could be used to manage or mitigate the security challenges affecting smart environments and by extension a multi-hazard early warning system.

Figure 1: Encompassing technologies making up the 4IR Technology.

2. RELATED WORKS

Devices in smart environments connected wirelessly or wired; are designed to utilize low power and their size is miniature (FIGURE 2); this results in low computing and minimal storage capabilities leading to resource constraints.

The ever-increasing gathering and transfer of data in smart environment networks, coupled with the potential transmission of this data to other wired or wireless networks, are an issue of concern in regard to security, authenticity and privacy. These concerns must be addressed in depth in order to fully leverage the benefits of smart environment networks. Communication via the Internet of Things (IoT) that is secure and private, presents numerous issues for smart environments. This is based on the notion that data gathered from IoT devices such as sensors, contain sensitive information, [3]. The authors further state that Blockchain's decentralized nature is viewed as the next generation of data security and that Blockchain is a revolutionary invention that has transformed electronic transactions and data preservation.

A review of the literature on blockchain, information security, and related mechanisms and frameworks was undertaken between 2000 and 2024 by [4]. TABLE 1 details the study fields, keywords, and corresponding researchers.

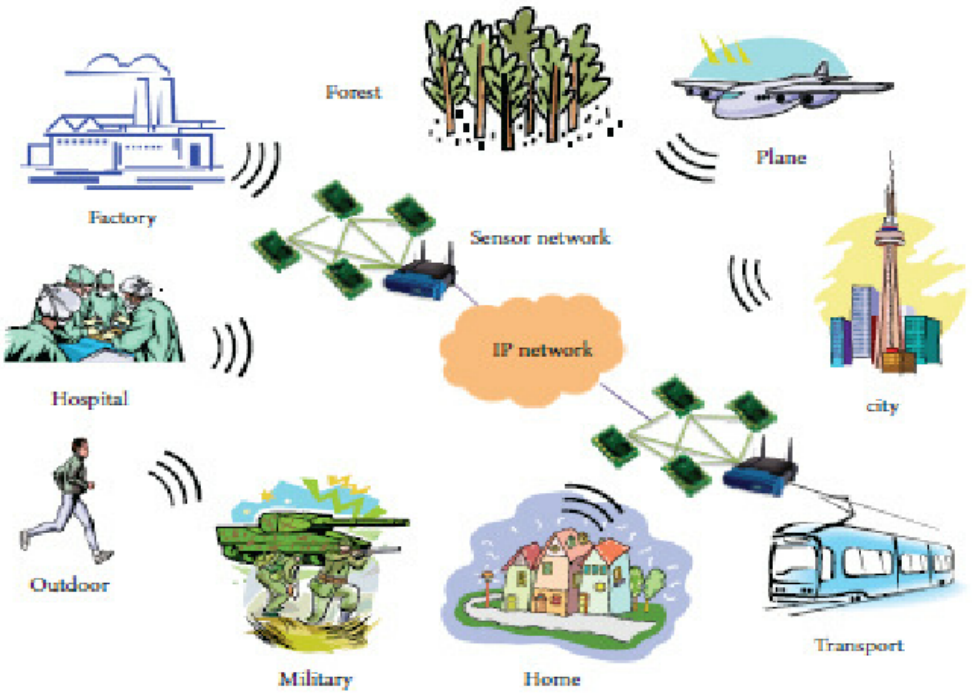

Figure 2: Smart environment topology. [5]

Blockchain has the potential to address the critical security vulnerability issues of information systems, particularly on data integrity and reliability or in applications that require extra trust guarantees

Table 1: Comparative analysis of related works

Scholar	Field	Methods and paths
Wang Tao (2023); Li Huanhuan (2021); Liu G (2016); Cui Chuanjian (2017)	Public Information and Cybersecurity	Virtual network, multi-dimensional authentication zero trust
Zhang Yifeng (2019); Li Wenjuan (2018), Lian Yuming (2022), Ma Chao (2023)	Network trust	Single sign-on and authentication
Du Jun (2023); Chen Li (2010), Liu Xun (2021)		CA/PKI/PMI application
Xu Yanhui (2023); Zhang Shunmei, Wei Shaojie (2007)		Trust Assessment BTMS Network ID
Li Yi, Feng Nan & Tan Shuncheng (2019); Khan A (2022); Gao S (2019); Li D (2017)		cross-domain data exchange
Khan A (2022); Gao S (2019); Li D (2017)		big data, blockchain, privacy
Li Weigang, Li Qiang (2021); Shang Kelong, Gu Qiang (2020); Wu Qi (2021)	Zero Trust Network	Dynamic Authentication, Encryption and Decryption \ Zero Trust Security
Li Qiang (2016); Zhang Yq (2024)	open network	trust relationship, transitive computational model
Chen Y, Zhang K (2024); Popa M, Fu Yx WnagL (2023)	Network Trust virtual robots	Trust management model, Trust measurement
Pang Jie, Tu Xuyan (2010); Xu Guangquan (2020)	Network Trust	Trust management, virtual robots
Singh M, Koprov P, Strauss S (2023); Upadhyay, S (2022)	Biometric Authentication	Face, fingerprint, iris, etc.

[6]. It has also been proven to addresses three types of risks: sample volatility, latency, and bias by [7].

In the past few years, there has been a significant increase in the use of Blockchain technology for security and privacy in information systems, the Internet of Things (IoT), healthcare, and cloud services. This growth is largely attributable to Blockchain's capacity to secure data using cutting-edge encryption techniques, decentralization, Immutable Ledger, and Smart Contracts. Reference [8], developed a model for ICT e-agriculture systems with a Blockchain infrastructure for use at the local and regional scale, with a focus on the specific technical and social requirements of Blockchain technology for protecting ICT e-agriculture systems. Reference [6], investigates the intentional use of Blockchain technology for data validation, data storage, data security, and data transfer to create decentralized, effective, fault-tolerant, and interoperable e-agriculture information systems. Reference [9], suggests a paradigm that makes use of smart contracts to guarantee reliable communication between devices and sensors. The authors of [10], conducted a survey that provides comprehensive reporting on various Blockchain studies and applications put forth by the research community, as well as their respective effects on Blockchain and its use across other applications or scenarios; their findings showed that Blockchain is increasingly being used in contemporary cloud- and edge-computing paradigms.

3. METHODOLOGY

This case study adopts already developed EWS; ITIKI: bridge between African indigenous knowledge and modern science of drought prediction [11], and Adaptive Environmental Management System (AEMS) for Lejweleputswa, Vhembe, and uMgungundlovu district municipalities [12].

ITIKI (Information Technology and Indigenous Knowledge with Intelligence) infrastructure is a novel approach that combines indigenous knowledge with contemporary ICT to give smallholder farmers in Africa access to useful agricultural information, especially weather forecasts. Through the use of both conventional and scientific weather prediction techniques, the goal is to increase agricultural output and resistance to climate forecast.

ITIKI Framework is made up of data collection and data processing and analysis.

The ITIKI Framework is comprised of the following components [13]:

- Indigenous Knowledge – Which focuses on the local populations' historic knowledge of weather patterns and how to deal with them.
- Effective Drought Index - calculates the degree of droughts by utilizing total precipitation as a weighting function of time and provides the Available Water Resources Index.
- Wireless Sensor Networks – Used to capture weather parameters at micro-level
- Mobile Phones – Used by farmers to access the eapplications
- Artificial Intelligence - To construct an integrated system capable of managing several moving pieces at both macro and micro levels, reasoning was required. The use of intelligent agents is used to accomplished this.

Core Infrastructure Components of ITIKI

Data Collection methods: ITIKI makes use of a variety of data sources, including meteorological satellites, weather stations, and indications derived from traditional knowledge. Observations of animal behaviour, plant phenology, or astronomical phenomena; all of which the local community has long utilised to predict the weather and can serve as indicators of indigenous knowledge.

Data Processing and Analysis: Data Processing and Analysis: Machine learning and artificial intelligence (AI) techniques are used to process and analyse the gathered data. To provide precise weather forecasts, the system combines measurements from the present with previous weather trends. To improve the forecast's accuracy and applicability to the area, indigenous knowledge is digitalized and incorporated into the model.

Using a participative approach through the Fuzzy Cognitive Maps (FCM) framework and infrastructure, the Adaptive Environmental Management System for the Lejweleputswa District is an innovative way to tackling difficulties related to sustainability and environmental management in this region. With this method, stakeholders who are directly impacted by environmental choices are included in the participatory process while yet maintaining the flexibility and adaptability of

adaptive management. Through the perspectives and expertise of various stakeholders, it further improves the capacity to model and comprehend complex ecological and social systems by incorporating the Fuzzy Cognitive Maps framework.

These MHEWS utilize unsecure communication channels during the transmission of dataset from legacy endpoints and sensors to the central repository, this is seen as a major vulnerability which needs to be addressed. This paper proposes the application of Blockchain to secure the vulnerability of data pipelines and Kubernetes to deploy and manage applications as a microservice in a containerized environment. Data collected by sensors is sent to different actors such as scientists, meteorologists, government agencies and the population at large. This paper aims to ensure that the disseminated information has not been tampered with and is in its original state.

Blockchain – a Distributed Ledger Technology (DLT), which is decentralized, will be implemented in a cloud environment using Kubernetes and on premise environment using Dockers [14].

FIGURE 3 depicts components necessary for the implementation of blockchain.

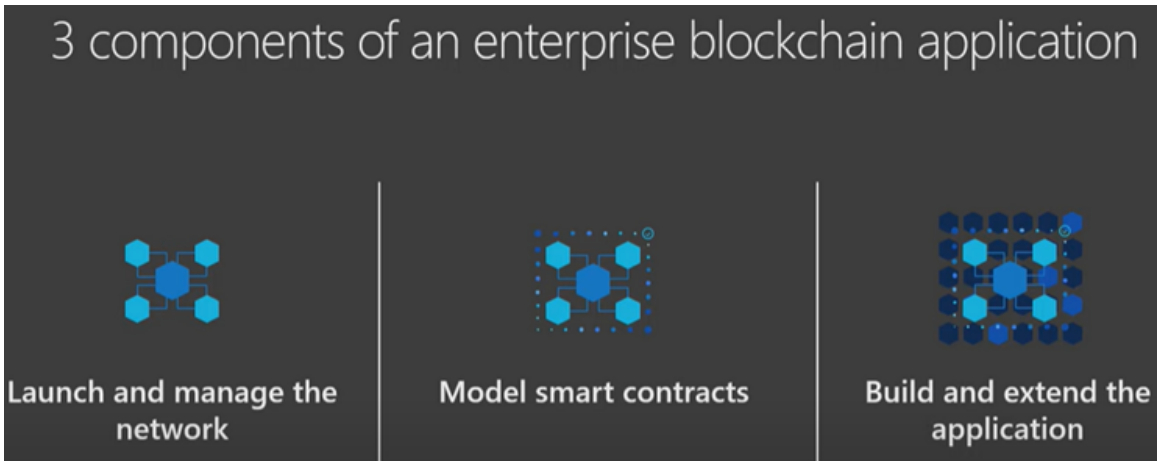

Figure 3: Overview of Blockchain application component.

The sensing nodes of the EWS and MHEWS will record, transmit, view, and modify transactional data that is encrypted onto their Blockchain based on the data transmission framework to be developed [15]. This process will create trust while also maintaining a high level of data integrity. In essence, the distributed nature of Blockchain provides no “hackable” entrance or point of failure that detrimentally exposes the entire datasets [16].

The adopted EWS consists of sensors, radio satellite, mobile phones, data transmission medium, repository/database and the processing unit [17]. The data is collected from sensing devices of the EWS for processing and dissemination via wired or wireless connections, making the data susceptible to manipulation. The study explores the implementation of the proposed Blockchain solution to address the security vulnerabilities. A consideration is the use of Azure Kubernetes Service (AKS) for the containerized deployment of EWS digital infrastructure. The systems will be deployed and managed as a containerized application in the cloud.

The implementation of Blockchain technology for data security can be a complex process, herein the processes adopted are simplified and broken down into several steps:

I Define the use case: This first step involves the identification of the specific data or information that needs to be secured and how it will be used, followed by the specific business logic and conditions that need to be encoded into the smart contract. In the study - case of environmental monitoring systems, the minimum and maximum readings of the measured parameters are noted as conditions/rules encoded into the smart contract. For example, early warning indicators such as temperature can have low and high values of -50celsius to +50celcius respectively.

II Choose a Blockchain platform: There are several Blockchain platforms that supports smart contract functionality, such as Ethereum or EOS with functionality that offers a complete end-to-end solution for developing, hosting, and managing Blockchain solutions. In a hybrid model design that allows data transmission to an online repository, the use of such services in Azure Cloud Security, which is best in class keeps both processes and data secure [18]. Azure Blockchain service supports Ethereum, Quorum Ledger, Corda, and Hyperledger Fabric.

This research employs Microsoft Confidential Ledger (ACL), a managed and decentralized ledger for data entry that is supported by Blockchain. Data committed to the Confidential Ledger is made tamperproof in perpetuity by ACL through consensus-based replicas and cryptographically signed blocks, prohibiting intentional or unintentional data alteration [19].

III Writing the smart contract code: Blockchain, such as Ethereum, allows the creation and execution of smart contracts. These contracts are written in code and stored on the Blockchain, making them transparent and secure. The business logic and conditions are coded using a programming language, such as Solidity.

IV Test and deploy the smart contract: Test the smart contract using a virtual environment, such as a Remix IDE, to ensure that it functions as intended. Deploy the smart contract to the Blockchain network, making it available for execution.

V Monitor and maintain: Monitor the network for any security breaches and perform regular maintenance to ensure the network remains secure.

Kubernetes (AKSs) is open-source container orchestration tool developed by Google that helps manage apps made of thousands of containers in different environments, [20]. It guarantees high availability where the application is always available to users and it is scalable and supports disaster recovery – if data is lost in the server, there is need to recover the data, meaning it has to be stored somewhere.

AKS offers serverless Kubernetes, creating an integrated continuous integration and continuous delivery (CI/CD) of data flows from the IoT sensing devices of the EWS to the centralized repository and processing applications in the cloud. Adding a full CI/CD data pipeline to the AKS clusters with automate securing of the datasets, detect failures early and optimizes pipelines with deep traceability to monitor security vulnerabilities.

The data protection through Kubernetes workloads with Blockchain containers will protect data flows, data-in-use, and code and data integrity of the consuming applications in the form of smart contracts. The consuming application on top of the ledge network write messages (data) to the ledger and read messages of it and route to consuming application and databases. The proposed Blockchain structure solution in place will guarantee the security of the critical datasets and reduce the security vulnerability of the MHEWS. For an on-premises solution, the study proposes the deployment of the smart environment – EMS will be localized, and data flows are monitored and routed from the sensing devices to the processing application/repository through the containers in a virtualized environment.

For the purpose of this study, Minikube was chosen as the orchestration platform to perform testing on sample data. FIGURE 4 shows how Blockchain will be implemented. Hyperledger Fabric as a permissioned Blockchain is the Blockchain technology that will protect datapipeline on-premise and one the cloud that will allow for a permissioned Blockchain with immediate finality.

4. EXPERIMENTS AND RESULTS

The aim of the paper is to implement blockchain in an effort to protect the datapipeline of the identified MHEWS. The objectives of the paper are as follows: identifying security challenges and vulnerabilities from the adoption of 4IR technologies in a MHEWS in the form of risk assessment; developing a secure data pipeline framework for MHEWS using blockchain technology to secure data transmission from the sensing devices to the repository or processing unit, lastly, it will test and evaluate the extent to which the application of blockchain technology is efficient in preventing the security vulnerabilities associated with 4IR technologies in a MHEWS. It will adopt two systems as stated before.

The two systems' integrated approach, together with the architecture's scale and complexity, improves environmental management's capacity to handle complexity and unpredictability. These qualities provide security issues that need to be addressed. This study proposes the use of Blockchain technology to mitigate the inherent security issues; in particular, protecting the datapipeline with the incorporation of Hyperledger Fabric framework.

4.1 Components of Mult Hazard Hazard Early Warning System

MHEWS usually include a number of essential components. Below are components as discussed by [21]:

i Hazard monitoring and detection – MHEWS uses different technology such as sensors, weather satellites, and rainfall gauges to monitor and identify potential threats is known.

ii Hazard assessment and analysis - It involves determining how possible effects of hazards may affect people, property, and the environment.

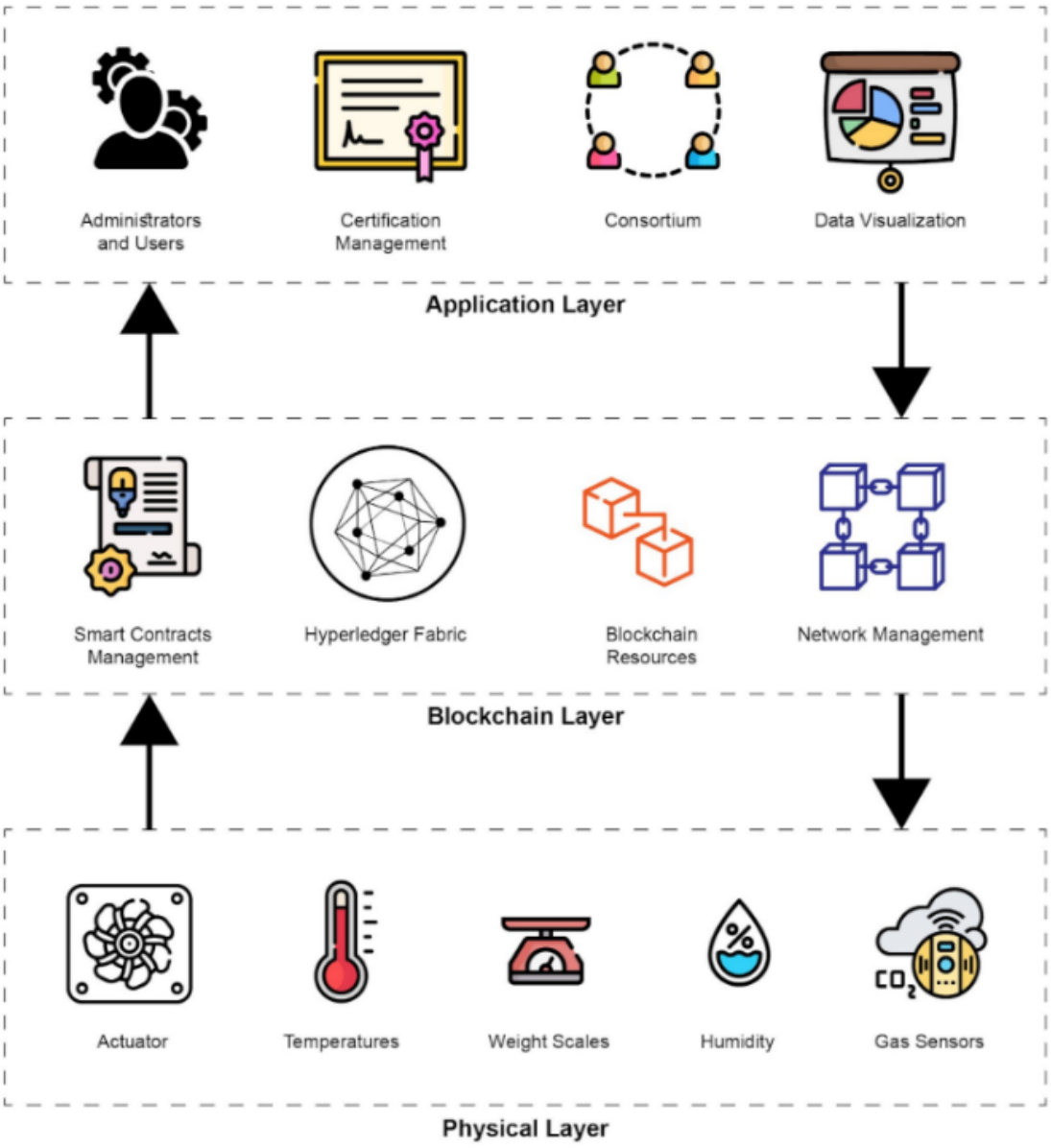

Figure 4: Overview of the Blockchain implementation framework.

iii Warning Communication: Using a variety of communication channels to inform authorities, emergency personnel, and the affected public of impending dangers in a timely and accurate manner.

iv Planning for readiness and Reaction: Creating and executing plans for readiness and reaction that are adapted to particular risks and regional conditions.

v Community Education and Engagement: Creating awareness, developing skills, and encouraging community involvement in disaster preparedness and response initiatives.

4.2 Blockchain Implementation

Upon its inception, Blockchain has been linked to cryptocurrencies, but it is recently notable that a variety of sectors has adopted it due to its primary purpose of enhancing security. The ability of Blockchain technology to create safe, immutable records that are distributed via a computer network underpins its significance [22], which goes beyond its application in finance. The decentralized ledger technology ensures that data is transparent and immutable, which provides improved security by design, [23].

Ethereum and Hyperledger Fabric are two open-sourced blockchain systems that are utilized extensively. For the purpose of this research, Hyperledger fabric has been chosen as the blockchain of choice. The reason behind this decision is based on research by [24]; where a comparison was conducted between the two blockchain technologies. The results of the research concluded that The hyperledger fabric offers a wide range of expansion capabilities and makes it easier to acquire various services for the creation of blockchains. Ethereum showed vulnerability to threats as DAO and DoS attacks.

4.3 Hyperledger Fabric Setup

The Hyperledger Fabric is running on a *Dell Latitude 7400* within a windows subsystem for Linux, with the operating system being *Ubuntu version 22.04.02*. The test network available on the Hyperledger Fabric network as shown in FIGURE 5, was used to evaluate the effectiveness of the Hyperledger Fabric network in securing sample data. Chaincode was also created to manage agreements between members of the network. FIGURE 6 shows the deployment of the *Temperaturesensor.sol* smart contract in Remix.

Peers operate the distributed ledger protocol of the fabric. The fabric makes a distinction between two types of peers: A validating peer is a network node in charge of executing consensus, approving transactions, and keeping track of the ledger. A non-validating peer, on the other hand, serves as a middleman between clients (issuing transactions) and validating peers and validating peers. Transactions are not executed by a non-validating peer, although they may be verified by it, [25].

The smart contract is deployed and tested on a local server before deployment to the cloud in Remix testing environment as depicted in FIGURE 7.

5. CONCLUSION

The era of IoT has improved people lives significantly and has potential to advance more. This has brought about integration of devices to enable and create smart environments. This phenomenon as great as may be, has brought about security concerns to creators and users of the systems. As it stands, surfeit research has been conducted regarding security issues around the implementation of smart homes, smart pedagogy, smart cities and in holistic view; smart environments.

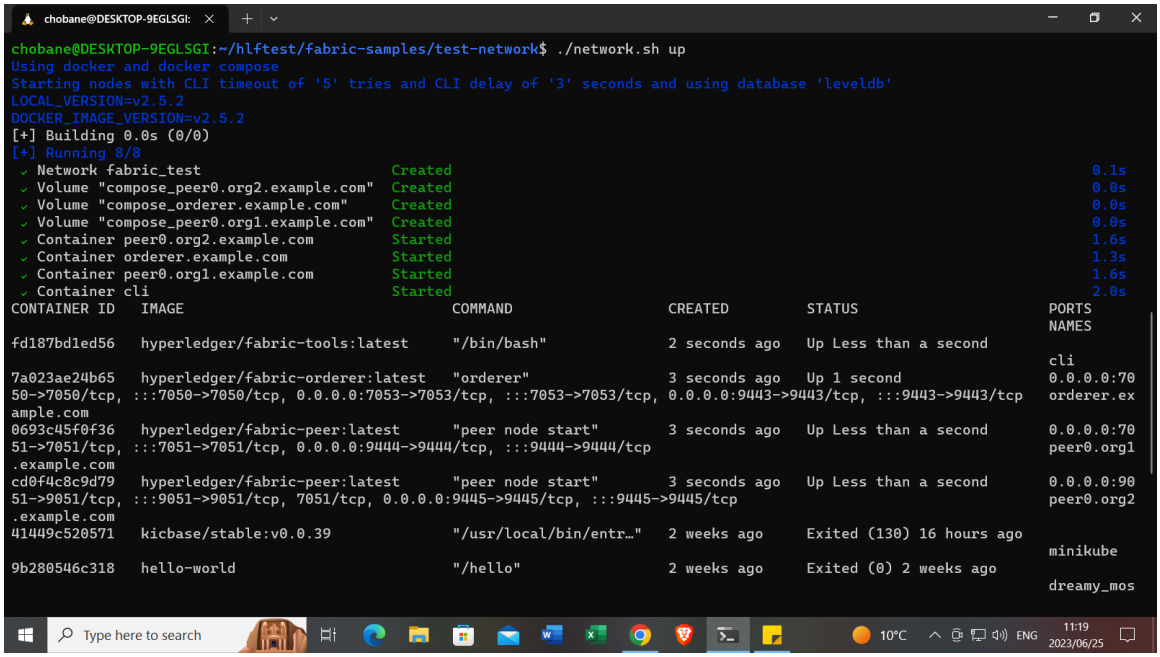

Figure 5: Network test-network up and running.

Figure 6: Using the Temperaturesensor.sol smart contract as an example in Remix for testing purposes.

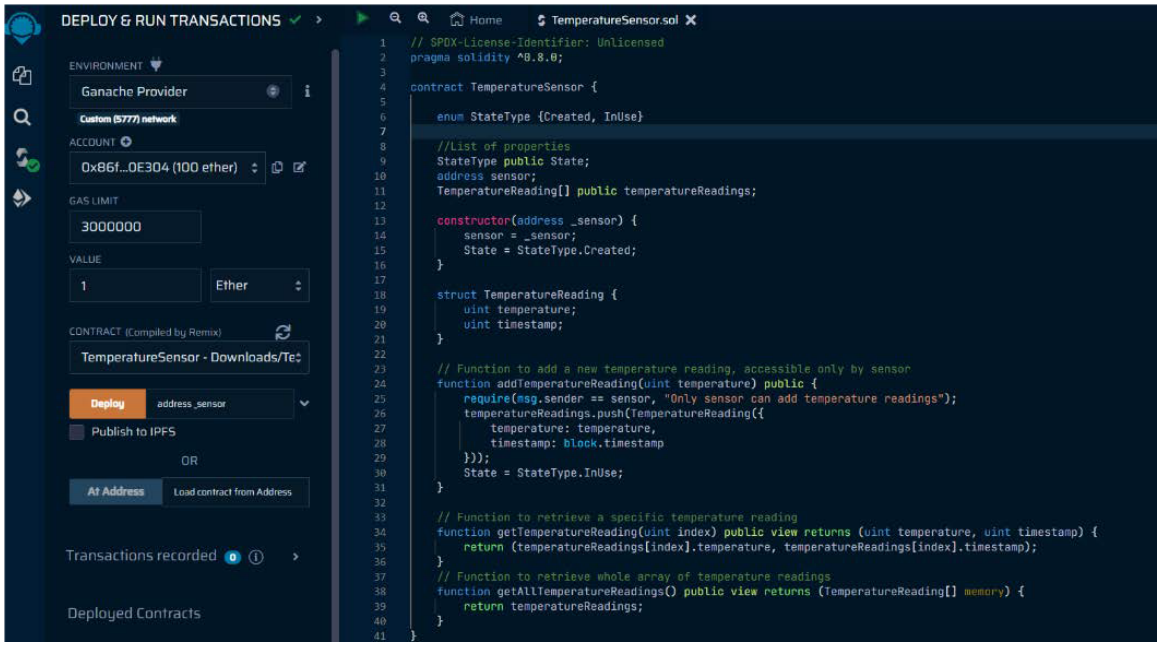

Figure 7: Deployment in Remix testing environment.

This study was aimed at mitigating security challenges facing the adoption and use of 4IR technologies, using a MHEWS as a caste study. The study adopts Blockchain and Kubernetes, two of the most transformative technologies of the last decade, using Blockchain to secure the vulnerably data pipelines and Kubernetes to deploy and manage applications as a microservice in a containerized environment. The application of these technologies present a powerful combination that helps component of an integrated MHEWS more secure, scalable, and decentralized. Overall, the integration of Blockchain and Kubernetes represents a significant step forward in the evolution of decentralized applications. It provides a new level of security, efficiency, and scalability that was previously impossible to achieve with traditional centralized systems. The study hypothesizes that Hyperledger Fabric can be used to protect the datapipeline of the MHEWS.

References

[1] Ullo SL, Sinha GR. Advances in Smart Environment Monitoring Systems Using IoT and Sensors. Sensors. 2020;20:3113.

[2] Scarfò A. The Cyber Security Challenges in the Iot Era. In: Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. Academic Press. 2018:53-76.

[3] Qashlan A, Nanda P, Mohanty M. Differential Privacy Model for Blockchain Based Smart Home Architecture. Future Gener Comput Syst. 2024;150:49-63.

[4] Wang F, Gai Y, Zhang H. Blockchain User Digital Identity Big Data and Information Security Process Protection Based on Network Trust. J King Saud Univ Comput Inf Sci. 2024;36.

[5] Aletà NB, Alonso CM, Ruiz RM. Smart Mobility and Smart Environment in the Spanish Cities. Transp Res Procedia. 2017;24:163-170.

[6] Daneshgar F,Sianaki OA, Guruwacharya P. Blockchain: A Research Framework for Data Security and Privacy. In: Barolli, L., Takizawa, M., Xhafa, F., Enokido, T. (eds) Web, Artificial Intelligence and Network Applications. WAINA 2019. Advances in Intelligent Systems and Computing. Springer, Cham.2019;927:966–974.

[7] Li X, Liang H. Blockchain Solution Benefits for Controlling Pandemics: Bottom-up Decentralization, Automation With Real-Time Update, and Immutability With Privacy Preservation. Comput Ind Eng. 2022;172:108602.

[8] Lin YP, Petway JR, Anthony J, Mukhtar H, Liao SW, Chou CF et al. Blockchain: The Evolutionary Next Step for ICT E-agriculture. Environments. 2017;4(3):1-13.

[9] Liao S, Wu J, Li J, Bashir AK, Yang W. Securing Collaborative Environment Monitoring in Smart Cities Using Blockchain Enabled Software-Defined Internet of Drones. IEEE Internet Things M. 2021;4:12-18.

[10] Berdik D, Otoum S, Schmidt N, Porter D, Jararweh Y. A Survey on Blockchain for Information Systems Management and Security. Inf Process Manag. 2021;58:102397.

[11] Masinde M. An Innovative Drought Early Warning System for Sub-Saharan Africa: Integrating Modern and Indigenous Approaches. Afr J Sci Technol Innov Dev. 2015;7(1):8-25.

[12] Mbele M, Masinde M. Development of Adaptive Environmental Management System: A Participatory Approach Through Fuzzy Cognitive Maps IST-Africa Week Conference. 2016;2016:1-13.

[13] Masinde M, Bagula A. ITIKI: Bridge Between African Indigenous Knowledge and Modern Science of Drought Prediction. Knowl Manag Dev J. 2011;7:274-290.

[14] Gourisetti SN, Cali Ü, Choo KK, Escobar E, Gorog C, Lee A et al. Standardization of the Distributed Ledger Technology Cybersecurity Stack for Power and Energy Applications. Sustain Energy Grids Netw. 2021;28:100553.

[15] Kim J, Li B, Scheideler OJ, Kim Y, Sohn LL. Visco-Node-Pore Sensing: A Microfluidic Rheology Platform to Characterize Viscoelastic Properties of Epithelial Cells. IScience. 2019;13:214-28.

[16] Arulprakash M, Jebakumar R. Towards Developing a Block Chain Based Advanced Data Security-Reward Model (Dseccs) in Mobile Crowd Sensing Networks Towards Developing a Block Chain Based Advanced Data Security- Reward Model (Dseccs) in Mobile Crowd Sensing Networks. Egyptian Informatics Journal. 2022;23(3):405-415.

[17] Akanbi, A. ESTemd: A Distributed Processing Framework for Environmental Monitoring Based on Apache Kafka Streaming Engine. Proceedings of the 4th International Conference on Big Data Research. 2020:18-25.

[18] Guerron X, Abrahão S, Insfran E, Fernández-diego M, González-ladrón-de-guevara F. A Taxonomy of Quality Metrics for Cloud Services. IEEE Access. 2020;8:131461-131498.

[19] Ramahlosi MN, Madani Y, Akanbi A. A Blockchain-Based Model for Securing Data Pipeline in a Heterogeneous Information System. 2024. Arxiv Preprint: https://arxiv.org/pdf/2401.09240

[20] Li Z, Zhang Y, Liu Y. Towards a Full-Stack DevOps Environment (Platformas-A-Service) for Cloud-Hosted Applications. Tsinghua Sci Technol. 2017;22:1-9.

[21] Ringo J, Sabai S, Mahenge A. Performance of Early Warning Systems in Mitigating Flood Effects. A review. J Afr Earth Sci. 2024;210:105134.

[22] https://bitcoin.org/bitcoin.pdf

[23] Swan M. Blockchain: Blueprint for a New Economy. ”O’Reilly Media. Inc. 2015.

[24] Mohammed, AH, Abdulateef, AA, Abdulateef, I. A. Hyperledger, Ethereum and Blockchain Technology: A Short Overview,” 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey. 2021:1-6.

[25] Cachin C, Schubert S, Vukolić M. Nondeterminism in Byzantine Faulttolerant Replication. Leibniz Int Proc Inform LIPIcs. 2017;70:24.1-24.16.